19-3809 BPG 19-3810 BPG

LOVELAND

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Christine D. Carlson, a Special Agent (SA) with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), being duly sworn, depose and state that:

1. I have been an Agent since June 1996. I began my career with the Immigration and Nationalization Service. I was assigned to the criminal alien program and as such have reviewed the contents of hundreds of Alien files (A-files). As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252 and 2252A. I have gained experience through training in seminars, classes, and daily work related to conducting these types of investigations. Specifically, I have received formal training through U.S. Customs, HSI, and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material, and internet crime. I have participated in the execution of numerous search warrants, which involved child exploitation and/or child pornography offenses. Many of the child exploitation and/or child pornography search warrants resulted in the seizure of computers, cell phones, magnetic storage media for computers, other electronic media, and other items evidencing violation of federal laws, including various sections of Title 18, United States Code, Section 2252A involving child exploitation offenses. I have also participated in the execution of numerous search warrants for online accounts, such as email accounts, online storage accounts and other online communication accounts related to child exploitation and/or child pornography. In the course of my employment with HSI, I have observed and reviewed numerous examples of child pornography

(as defined in 18 U.S.C. § 2256) in all forms of media including computer media and within online accounts.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and I am a law enforcement officer with the authority to affect arrests and execute warrants issued under the authority of the United States.

3. This affidavit is made in support of an application for warrants to search the following (hereinafter referred to as the "TARGET CELL PHONE 1 and TARGET CELL PHONE 2"):

a. The cell phone seized from Miguel Angel ZAMORA-Argueta, on October 7, 2019 ("TARGET CELL PHONE 1", more fully described on Attachment A-1, which is incorporated here by reference);

b. The cell phone seized from Miguel Angel ZAMORA-Argueta, on May 21, 2019 ("TARGET CELL PHONE 2", more fully described on Attachment A-2, which is incorporated here by reference);

4. The TARGET CELL PHONE 1 and TARGET CELL PHONE 2 are to be searched for evidence of violations of Title 8 USC § 1326 (a) (Reentry of Removed Alien). In addition, TARGET CELL PHONE 2 is to be searched for evidence of violations of 18 U.S.C. §§ 2422(b) (Enticement and Coercion of a Minor); 2252A(a)(5)(B) (possession of child pornography); 1470 (transfer of obscene materials) (the TARGET OFFENSES).

5. In addition to my own observations and investigative discoveries, the statements in this affidavit are based in part on information and reports provided by Immigration and Customs Enforcement Officials, including ERO Deportation Officer Paulysha Spratley, and the Baltimore County Police Department. The lead detective in the state case against ZAMORA-Argueta contacted me after the execution of the state search warrant and I assisted him to further the investigation and eventual state prosecution of ZAMORA-Argueta. Since this affidavit is being

submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES are located within the TARGET CELL PHONE 1 and within the TARGET CELL PHONE 2.

PROBABLE CAUSE

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

6. Based on my investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet to view and receive images of child pornography, or who communicate with others regarding sexual fantasies regarding children, or who solicit child pornography from minors, are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals, including the following:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, or in online storage, email accounts or other online communication accounts, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. This data is typically in digital format, and often maintained on computers and in online storage, email accounts or other online communication accounts.

f. Individuals who would have knowledge on how to distribute and receive digital images of child pornography through the use of Peer to Peer networks and other online methods would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

7. Based on my investigative experience related to computer and internet related child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned the following:

a. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies.) The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

b. The development of computers and the internet have added to the methods used by child pornography collectors to interact with and sexually exploit children.

c. Child pornographers can now transfer photographs from a camera onto a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography.

d. Child pornography can be transferred via electronic mail, text message applications, or through file transfer protocols (FTP) to anyone with access to a computer and modem, including for these purposes a cellular phone. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), easy access to the Internet, and online file sharing and storage, the computer is a preferred method of distribution and receipt of child pornographic materials.

e. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography use online resources to retrieve and store child pornography, including services offered by Internet Portals such as AOL Inc., Yahoo! and Google, Inc., Facebook, Dropbox, Instagram, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services, file exchange services, messaging services, as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Email accounts, online storage accounts, and other online communication accounts allow users to save significant amounts of data, including email, images, videos, and other files. The data is

maintained on the servers of the providers, and is occasionally retained by the providers after the user deletes the data from their account.

f. In my recent investigative experience, as well as recent discussions with law enforcement officers, I know that individuals who collect child pornography are using email accounts, online storage accounts, and other online communications accounts to obtain, store, maintain, and trade child pornography with growing frequency, in addition to, or as an alternative to, the use of personal devices.

8. Based on traits shared by collectors, the use of email, online storage accounts, and other online communication accounts, and the increased storage capacity of computers and server space over time, as well as the particular facts set forth below, there exists a fair probability that evidence regarding the reentry of a removed alien, the enticement and coercion of a minor and possession of child pornography will be found in the cell phones seized from ZAMORA-Argueta, notwithstanding the passage of time.

INVESTIGATIVE FACTS

9. The crime of illegal reentry 8 U.S.C. § 1326 generally requires the government to prove, beyond a reasonable doubt, that (1) the Defendant is an alien (not a citizen or national of the United States); (2) that the defendant had previously been deported/removed/excluded from the United States; (3) that after being deported/removed/excluded from the United States, the defendant reentered the United States; and (4) that the Defendant had not received the express permission of a qualified government official to apply for readmission. *See Sand & Siffert* 2 Modern Federal Jury Instructions-Criminal P 33A.06 (2019). Accordingly, the Defendant's identity is a critical issue in an illegal reentry case because the government must show that the Defendant was an alien, that the Defendant was present in the United States, and establish the Defendant's immigration history, including deportation(s)/removal(s)/exclusion(s), in order to prove the crime beyond a reasonable doubt.

10. Based on my training and experience, including my review of cell phone extractions

as part of investigations in other cases, a cell phone often contains information in the form of photographs, text messages, phone calls, emails, videos, and other items regarding the identity, whereabouts, place of work, contacts, family, life events, and travel of the cell phone's user or users. People often use their cell phones multiple times a day as an essential feature of their lives, and accordingly these pieces of information are often on cell phones, even for a cell phone that is used only briefly, and these pieces of information concerning the location, identity, associates, travel, and lifestyle of a given person, are directly relevant to the person's identity, which as discussed above, is a critical issue in illegal reentry cases. (8 U.S.C. § 1326(a)). For example, cell phones often contain "selfies" or other pictures of the cell phone's user, and these photographs would corroborate a person's identity, for example, by comparison to the person's appearance in photographs contained within an Alien file. Photographs on a cell phone also often include people other than the phone's user, such as friends, family, or associates, which may be corroborative of identity if for example the photograph includes a person's family members or known associates. As another example, messages, whether a text message, or through an application on a cell phone, between a phone's user and family members or known associates are also corroborative of a cell phone user's identity. Messages may also contain substantive conversations that corroborate a person's identity, their travel, their whereabouts, etc., all of which goes to the user's identity and which can be used to corroborate the Defendant's alienage, presence in the United States, nationality, and travel. Also corroborative of identity are any electronic accounts, calendar entries, e-mail accounts, videos, and other media. As a basic example, cell phones often contain a person's name in numerous locations, for example, in electronic account information, in messages between the cell phone's user and others, in e-mail communications located on the phone, in photographs or other media on the phone, etc. iPhones such as TARGET CELL PHONE 1 and TARGET CELL

PHONE 2, allow the cell phone user to give the iPhone a "name" which may contain the cell phone user's name or other information corroborative of identity. Cell phones also often contain contact information for friends, relatives, and known associates, which again, can be used to corroborate a person's identity. Cell phones also often contain information concerning the user's location, either through applications that directly relate to a user's location, such as GPS or map type locations; or through substantive communications about a user's location; or through information contained in other media forms, for example, pictures or videos of certain recognizable locations; or through "metadata" that may record information for media (such as a video or picture) that establishes, among other things, when and where the media was created. Such evidence is relevant to corroborating immigration events, such as the timing of deportations/removals, the timing of a person's reentry, or a person's presence within the United States.

11. Miguel Angel ZAMORA-Argueta ("ZAMORA-Argueta"), DOB: 06/01/1994, is a citizen of El Salvador. ICE is currently in possession of a copy of ZAMORA-Argueta's El Salvadoran passport. ZAMORA-Argueta first came into contact with United States Immigration on May 5, 2014 when he was arrested by the United States Border Patrol Officers (USBP) at or near Hebbronville, Texas. ZAMORA-Argueta was taken into custody and processed for Expedited Removal under the Provision Section 235 (b)(1) of the Immigration and Nationality Act. ZAMORA-Argueta was removed to El Salvador on June 9, 2014 through Brownsville, Texas as evidenced by a signed and fingerprinted I-296 (Notice to Alien Ordered Removed/Departure Verification) in ZAMORA-Argueta's Alien File.

12. On October 7, 2019, ERO Deportation Officer Paulysha Spratley read ZAMORA-Argueta his *Miranda* Rights and he waived those rights. Those rights were also shown to him on a form that displayed them in both Spanish and English. Subsequently ERO Deportation Officer

Spratley took a sworn statement from him. According to a sworn statement given and signed by ZAMORA-Argueta, he reentered the United States by crossing the border. ZAMORA-Argueta was asked, "Were you deported from the United States? When? Where?" in the English language. The response was recorded as: "Yes about 6 years ago" (approximately 2014). ZAMORA-Argueta was subsequently asked "Did you illegally enter the United States? When? Where? How?" in the English language. The response was recorded as: "Yes, after I got deported, I came back because of the gangs. When I was in El Salvador, I paid a coyote half of $8500 and when I got to Texas, I paid the other half".

13. According to a probable cause statement from District Court of Maryland for Baltimore County (Case#19-111-1071), a search warrant affidavit, and per conversations with Baltimore County law enforcement officials, on various dates in 2019, ZAMORA-Argueta engaged in inappropriate telephone messaging conversations with a minor female (11 years old). The minor's father reported the incident to Baltimore County Police. During interviews with Baltimore County law enforcement, the minor victim admitted to sending ZAMORA-Argueta nude photographs of herself. The minor further stated that ZAMORA-Argueta requested sexual contact with her. A Baltimore law enforcement officer observed numerous communications on the victim's phone on the Snapchat application between the minor victim and a user identified as "BF-jackson-zamora" that contained, among other things (1) a photo of a white Toyota Tundra matching in appearance a truck observed at ZAMORA-Argueta's residence; (2) a photo of ZAMORA-Argueta; (3) numerous photos of the minor victim, including nude photos exposing the victim's breasts, vaginal area, etc., some with the minor victim's face visible and some without; and (4) messages from BF-jackson-zamora to the minor victim asking the minor victim to touch herself.

14. On May 20, 2019, the Honorable Judge Karen A. Pilarski, District Court of Maryland for Baltimore County authorized a search and seizure warrant for ZAMORA-Argueta's residence located at 327 Endsleigh Avenue, Middle River, MD 21220. On May 21, 2019, the aforementioned search and seizure warrant was executed. During execution, ZAMORA-Argueta identified a gold in color iPhone located next to his bed in the upstairs front bedroom as belonging to him: TARGET CELL PHONE 2. An on-scene forensic preview of ZAMORA-Argueta's iPhone revealed a Snapchat account with the profile name jackson-zamora. Detectives interviewed ZAMORA-Argueta in private and the interview was audio recorded. ZAMORA-Argueta was read his *Miranda* rights for a second time and agreed to speak with detectives. ZAMORA-Argueta admitted to knowing the victim and creating a Snapchat account with the username jackson-zamora before requesting a lawyer. ZAMORA-Argueta was arrested by the Baltimore County Police Department and charged with (1) Two Counts of Child Porn Permit Sex Subj and (2) Two Counts of Child Porn Solicit Subject. TARGET CELL PHONE 2 was seized by Baltimore County Police and inventoried as evidence. On September 25, 2019, ZAMORA-Argueta was convicted in the Circuit Court of Baltimore County, MD of Child Porn Solicit Subject and was sentenced to 10 years' incarceration all suspended but time served. ZAMORA-Argueta was released to the community on September 25, 2019. ZAMORA-Argueta's property, including TARGET CELL PHONE 2, was still in the possession of the Baltimore County Police Department as it was contraband and evidence of the crime for which ZAMORA-Argueta was convicted.

15. On October 7, 2019, ZAMORA-Argueta was identified by Immigration and Customs Enforcement (ICE) Task Force Officers at approximately 1100 hours outside of the Division of Parole and Probation: 8914 Kelso, Drive, Essex, MD 21221 while attempting to enter a White Toyota Tundra, bearing Maryland license plate 7DH2819, which is registered to

ZAMORA-Argueta. At this point, ZAMORA-Argueta was identified and apprehended. During apprehension, an ICE Officer seized a rose gold colored cell phone (TARGET CELL PHONE 1) from ZAMORA-Argueta's person. TARGET CELL PHONE 1 is similar in appearance to TARGET CELL PHONE 2. *See* Attachments A-1 and A-2. As part of normal ICE detention procedures, ZAMORA-Argueta's personal property was placed into a plastic property bag when he was taken into custody and transported to the Baltimore Field Office.

16. On October 7, 2019, ZAMORA-Argueta and his property (including TARGET CELL PHONE 1) was transported to Worcester County Detention Center for housing. On October 24, 2019, ZAMORA-Argueta and his property (including TARGET CELL PHONE 1) was transported to the Baltimore Field Office. At this time, a Deportation Officer retrieved TARGET CELL PHONE 1 and placed it into an evidence bag.

17. Cell phones are contraband and detained aliens are not permitted to have cell phones during their detention. ICE policies and procedures permit detained persons to designate a specific person or persons to retrieve their property. If a designated person had requested ZAMORA-Argueta's cell phone between October 7, 2019 and October 24, 2019, consistent with ICE policies and procedures, the cell phone would have been released to that person. A review of ZAMORA-Argueta's file from his detention failed to find documentation indicating that any person was designated to retrieve property. In fact, a form filled out on October 7, 2019, which inventories ZAMORA-Argueta's property including TARGET CELL PHONE 1, asks the detainee whether the detainee will (1) personally pick up their property upon release from detention, (2) designate someone to pick up their property, or (3) abandon the property. (EXHIBIT 1). The form lists these three options both in the Spanish and English languages. The completed form includes ZAMORA-Argueta's initials next to the option (in the Spanish language portion) indicating that

ZAMORA-Argueta will personally pick up his property. The portion of the form allowing the detainee to list the name and contact information for a designated person (option 2) to pick up their property is blank both in the Spanish and English language sections. The form includes ZAMORA-Argueta's signature just beneath where option 1 is indicated and initialed. Later on in the form, there is a place where the detainee can designate an emergency contact. Two names, with corresponding cell phone numbers, are listed there as emergency contacts.

18. On October 30, 2019, Deportation Officer Spratley confirmed with a Baltimore County detective that they still had possession of TARGET CELL PHONE 2. On October 31, 2019, Deportation Officer Spratley retrieved ZAMORA-Argueta's property from the detective including TARGET CELL PHONE 2 and other identification documents. The property was placed in a sealed evidence bag.

19. TARGET CELL PHONE 1 and TARGET CELL PHONE 2 are both iPhones. *See* Attachments A-1 and A-2. iPhones, as with other Apple devices, use the service iCloud, which allows users to store files on Apple's servers in order to sync their files across all of their Apple devices, including iPhones such as TARGET CELL PHONE 1 and TARGET CELL PHONE 2. According to iCloud's terms and conditions, at http://www.apple.com/legal/internet-services/icloud/en/terms.html ,[1] "iCloud Backup periodically creates automatic backups for iOS devices". Another part of Apple's website, https://support.apple.com/guide/mac-help/what-is-icloud-mh36832/mac , explains "iCloud securely stores your photos, videos, documents, music, apps, and more—and keeps them updated across all your devices". And iPhone users can use the iCloud Backup feature to "Transfer your personal data and purchased content to your new devices using your previous device's iCloud backup." (https://support.apple.com/en-us/HT210217). Accordingly,

[1] All website references included herein are current as of November 19, 2019.

19-3809 BPG

19-3810 BPG

even iPhone devices used for a relatively short amount of time, such as may be the case with TARGET CELL PHONE 2, can contain a wealth of information predating a user's use of the iPhone and stretching back to previous use of other Apple devices.

20. On October 30, 2019, a federal grand jury for the District of Maryland returned a one-count indictment against ZAMORA-Argueta charging him with 8 U.S.C. § 1326(a) (Reentry after Removal).

CONCLUSION

21. Based on the foregoing information, I respectfully submit that I have probable cause to believe that contraband, and evidence, fruits, and instrumentalities of the TARGET OFFENSES are located within TARGET CELL PHONE 1 and TARGET CELL PHONE 2 as described in Attachments A-1 and A-2. I therefore respectfully request that search warrants be issued authorizing a search of the TARGET CELL PHONE 1 and TARGET CELL PHONE 2 and authorizing the seizure and examination of any such information or items of evidentiary value found therein as described in Attachments B-1 and B-2.

Christine D. Carlson
Special Agent
Homeland Security Investigations

Sworn and subscribed before me
this 22ND day of November, 2019

HONORABLE [redacted]
UNITED STATES MAGISTRATE JUDGE

Beth P. Gesner
United States Magistrate Judge

19-3809 BPG 19-3810 BPG

EXHIBIT 1

U.S. Immigration and Customs Enforcement

Name:	AR#:	DOB:	Nationality:
ZAMORA-ARGUETA, MIGUEL	206 708 742	06-01-1994	ELSAL
I-77: 4075765	G-589:	Funds: $ 31.00	Date of Action: 10/7/2019

Inventory of Property / Inventario de Propiedad

	Backpack			Cellphone charger			Luggage			Rings		
	Belt ~ BLK	1		Chain/ Necklace			Keys			Shoe Laces	2	Brown
	Bible			Earrings			Medication			Shoes/Boots		
	Bracelet			Eyeglasses			Personal Papers			Watch		
	Cellphone T-MOBILE	1		Jacket			Purse			Wallet BLK	1	

Gang affiliation: YES ☐ NO ☒ _____ Medical issues: YES ☐ NO ☒ _____

Arresting & Certifying Officer: DO/TPO Johnson BK 4644

The detainee, by signing below certifies the accuracy of the inventory and turns the property over to ICE for safekeeping. Any missing or damaged items must be noted on a separate piece of paper. **Detainee property will be deemed "ABANDONED" 30 days after subject's release from custody in accordance with applicable ICE policies and procedures (SEE DETAINEE MANUAL).**

CHECK ONE OF THE FOLLOWING CHOICES:

_____ 1. I will personally pick up my property.

_____ 2. Please release or contact the following to pick up my property _____

Tel:_____

_____ 3. Pursuant to the provisions of Title 41, Code of Federal Regulations, Part 101-48.001-8, I hereby abandon all claims to the above described articles, and waive any further rights of proceedings relative to said property.

Detainee Signature: _____ Date: _____

El detenido, al firmar a continuación, certifica la precisión del inventario y entrega la propiedad a ICE para su custodia. Cualquier artículo perdido o dañado debe anotarse en una hoja de papel por separado. **La propiedad del detenido se considerará "ABANDONADA" 30 días después de que el sujeto ha sido puesto en libertad de acuerdo con las pólizas y procedimientos de ICE (VER MANUAL DE DETENIDOS).**

MARQUE UNA DE LAS SIGUIENTES OPCIONES:

MZ 1. Recogeré personalmente mi propiedad.

_____ 2. Por favor, liberen o contacten a la siguiente para recoger mi propiedad a _____

Tel:_____

_____ 3. De conformidad con lo dispuesto en el Título 41, del Código de Regulaciones Federales, Parte 101-48.001-8, por la presente abandono toda reclamación sobre los artículos descritos anteriormente, y renuncio a cualquier otro derecho relativo a dicha propiedad.

Firma Del Detenido: _____ Fecha: 10/7/2019

RECEIPT OF DETAINEE HANDBOOK/ RECIBO DEL MANUAL DE DETENIDOS: _____

Emergency Contact / Contacto de Emergencia:

Name/Nombre: Liset Lopez Tel: 443 522-5902 Relation/Relación: Wife

Blue Floor Officer:

Verifying Officer: _____ Date/Time: _____

PABLO ARGUETA 443 527-1382

ZAMORA

I&P V2

19-3809 BPG

ATTACHMENT A-1

DESCRIPTION OF ITEM TO BE SEARCHED

The iPhone depicted below seized from Miguel Angel ZAMORA-Argueta, on October 7, 2019, is currently being held at ICE, 31 Hopkins Plaza, Baltimore, MD 21201:

Rose Gold Colored Apple iPhone

ATTACHMENT B-1
ITEMS TO BE SEIZED

All records contained in the items described in Attachments A-1, which constitute evidence of violations of 8 USC § 1326 (a), as outlined below:

1. All information in the form of photographs, text messages, phone calls, emails, videos, and any other items that bear on the identity, travel, nationality, immigration history, and contacts of the cell phone's user or users.

2. Any and all records related to the location of the user(s) of the devices.

3. For the Device:

    a. Evidence of who used, owned, or controlled the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

    b. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

    c. evidence of the lack of such malicious software;

    d. evidence of the attachment to the Devices of other storage devices or similar containers for electronic evidence;

    e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the Devices;

    f. evidence of the times the Devices were used;

    g. passwords, encryption keys, and other access devices that may be necessary to access the Devices;

h. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Devices;

i. contextual information necessary to understand the evidence described in this attachment.

4. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possible recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

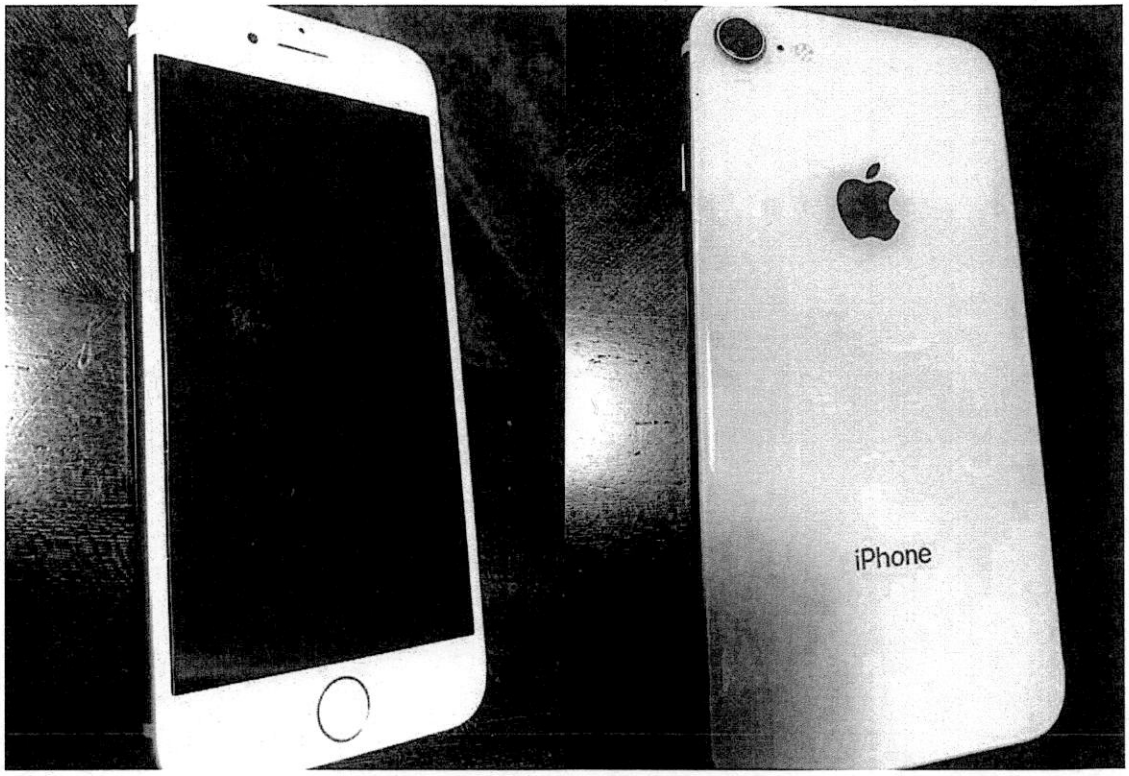
5. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory,

file or storage area, shall cease.

ATTACHMENT A-2

DESCRIPTION OF ITEM TO BE SEARCHED

The iPhone depicted below seized from Miguel Angel ZAMORA-Argueta, on May 21, 2019, is currently being held at ICE, 31 Hopkins Plaza, Baltimore, MD 21201:



Rose Gold Colored Apple iPhone

19-3810 BPG

ATTACHMENT B-2

ITEMS TO BE SEIZED

All records contained in the items described in Attachments A-2, which constitute evidence of violations of 8 USC § 1326 (a) and 18 U.S.C. §§ 2422(b) (Enticement and Coercion of a Minor); 2252A(a)(5)(B) (possession of child pornography); 1470 (transfer of obscene materials), as outlined below:

1. All information in the form of photographs, text messages, phone calls, emails, videos, and any other items that bear on the identity, travel, nationality, immigration history, and contacts of the cell phone's user or users.

2. Any and all records related to the location of the user(s) of the devices.

3. Any and all photographs, text messages, phone calls, emails, videos, applications, notes, documents, records, or correspondence pertaining to child pornography as defined under Title 18 U.S.C. § 2256(8).

4. Any and all correspondence identifying persons transmitting, receiving or possessing, through interstate commerce including by U.S. Mails or by computer, any visual depictions of minors engaged in sexually explicit conduct, including through Snapchat and other applications, as defined in Title 18 U.S.C. § 2252A(a)(5)(B) & (b)(2), 2256(2).

5. Any and all records, documents, invoices, and materials that concern any accounts with Snapchat, or any other Internet Service Provider applications, screen names, online accounts, websites, or email accounts.

6. Any and all visual depictions of minors, including depictions of minors engaged in sexually explicit conduct, nude pictures, and modeling.

7. Any and all diaries, notebooks, notes, address books, pictures, emails, chats, directions, maps, banking, travel, documents, and any other records reflecting personal contact and any other activities with minors.

8. Any and all financial documents, records, receipts, credit card statements, and/or correspondence relating to payments sent and/or received in connection with minors engaged in sexually explicit conduct, nude pictures, modeling, and/or hosting websites.

9. Image and video files that depict children engaged in sexually explicit conduct pursuant to Title 18 U.S.C. § 2256.

10. Any and all notes, documents, records, photos or correspondence that indicate a sexual interest in children, including, but not limited to:

    a. Correspondence with children;
    b. Any and all visual depictions of minors;
    c. Internet browsing history;
    d. Books, logs, emails, chats, diaries, and other documents.

As used above, the terms "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

11. For the Device:

    a. Evidence of who used, owned, or controlled the devices at the time items of interest were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the Devices of other storage devices or similar containers for electronic evidence;

e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the Devices;

f. evidence of the times the Devices were used;

g. passwords, encryption keys, and other access devices that may be necessary to access the Devices;

h. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the Devices;

i. contextual information necessary to understand the evidence described in this attachment.

12. With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

f. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

g. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

h. "scanning" storage areas to discover and possible recover recently deleted files;

i. "scanning" storage areas for deliberately hidden files; or

j. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

13. If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.